Jurnal Ilmiah Wahana Pendidikan, September 2026, 12 (9.B), 196-210
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/14277
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Inconsistency in the Application of the Electronic Information and Transactions Law to Online Fraud in Bandung City

Yudhi Jatnika[1] , Temmy Fitriah Alfiany[2]

[1,2] *Department of Law, Faculty of Law, Universitas Muhammadiyah Sukabumi*

Received: 02 Agustus 2026
Revised: 13 Agustus 2026
Accepted: 02 September 2026

Abstract

Law enforcement against online fraud in Indonesia continues to struggle with inconsistency in applying Law Number 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law (the EIT Law). Within the jurisdiction of Bandung City, only about 31.4% of 312 online fraud reports filed between 2021 and 2024 resulted in final and binding decisions, and the legal provisions applied varied considerably. This study analyzes the concrete application of the EIT Law at the indictment, evidentiary, and adjudication stages and identifies the factors driving such inconsistency. Adopting an empirical juridical (socio-legal) method with statutory and case approaches, the research draws on in-depth interviews with investigators, prosecutors, and judges, and on three Bandung District Court decisions examined through triangulation. The findings show that the application of the EIT Law is inconsistent: three substantively similar cases produced three distinct decision patterns, namely the sole application of the Criminal Code, the independent application of the EIT Law, and cumulative application. This inconsistency arises from four interacting factors: normative dualism between the Criminal Code and the EIT Law, the limited technical capacity of officials, weak institutional coordination and inadequate digital forensic infrastructure, and a legal culture favoring the Criminal Code. The study concludes that normative harmonization, technical guidelines from the Supreme Court and Attorney General's Office, strengthened digital forensics, and an objective and measurable model for determining the legal basis are required; the last constitutes the novelty of this research.

Keywords: EIT Law; online fraud; decision inconsistency; legal certainty; criminal liability.

(*) Corresponding Author: yudhijatnika@ummi.ac.id

How to Cite: YUDHI JATNIKA, Y., & Alfiany, T. (2026). Inconsistency in the Application of the Electronic Information and Transactions Law to Online Fraud in Bandung City. *Jurnal Ilmiah Wahana Pendidikan*, *12*(9.B), 196-210. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/14277.

INTRODUCTION

Indonesia's digital transformation has occurred on a massive scale. By 2023, the number of internet users had exceeded 212 million, roughly 77% of the population (We Are Social & Hootsuite, 2023), placing Indonesia among the largest digital markets in Southeast Asia. The migration of economic and social activity into cyberspace has expanded access and efficiency, yet it has simultaneously created new spaces for crime that conventional legal instruments struggle to reach. Online fraud fraud that exploits electronic media and the internet to induce a victim to surrender something of value (Moeljatno, 2022) has become one of the most disquieting and fastest-evolving forms of cybercrime.

Empirical data confirm this escalation. The National Police Criminal Investigation Agency recorded a 41.5% surge in cybercrime in 2022, with online fraud as the largest contributor (Bareskrim Polri, 2023), while in 2023 the Directorate of Cyber Crime received more than 8,831 reports of internet-based fraud (Direktorat Tindak Pidana Siber Bareskrim Polri, 2024). These figures likely represent only the tip of the iceberg: a high dark number persists owing to victims' unfamiliarity with reporting procedures, shame, and pessimism about the effectiveness of law enforcement.

The core problem lies not in the absence of norms but in the misalignment between the evolution of criminal modus operandi and the legal framework governing it. Indonesia's penal system rests on a Criminal Code inherited from the colonial era that was never designed for digital crime, whereas the EIT Law which specifically governs conduct through electronic media does not expressly use the term “fraud.” The result is a dualism: a single act of online fraud may simultaneously satisfy the elements of Article 378 of the Criminal Code and Article 28(1) of the EIT Law, with no clear rule specifying whether the provisions apply alternatively, subsidiarily, or cumulatively (Suhariyanto, 2020).

This dualism produces tangible inconsistency at the point of application. In Supreme Court Decision Number 2168 K/Pid.Sus/2019, the perpetrator of online sale-and-purchase fraud was convicted under Article 378 of the Criminal Code in conjunction with Article 28(1) of the EIT Law signaling judicial hesitation in drawing the boundary between conventional fraud and electronically mediated fraud. In Bandung City, the deviation is starkly visible in an investment-scam case (Bandung District Court Decision Number 131/Pid.B/2022/PN.Bdg): although charged cumulatively, the defendant was convicted under Article 378 alone, on the ground that the element of “disseminating false news” was not satisfied. The decision raises a critical question: why was the EIT Law the very statute designed for electronic crime set aside in a case that unfolded entirely in the digital realm?

The problem grows more acute because online-fraud techniques evolve far faster than legal institutions can adapt. From simple sale-and-purchase scams, fraudulent investment schemes, phishing, and romance scams, the modus has now extended to the use of generative artificial intelligence to produce deepfake content the falsification of the faces and voices of trusted figures which is far harder for lay victims to detect (Ramli, 2020). This diversification creates a classification challenge: officials are forced to map continuously mutating conduct onto relatively static norms. The normative tension is evident in the element “inducing another to surrender something” under Article 378, which presupposes direct causation and observable interaction a fragile assumption when the perpetrator operates from a different jurisdiction, uses a fabricated virtual identity, and manipulates victims through prolonged digital conversation.

A macro dimension reinforces the urgency. Concern over the security of digital transactions remains a principal obstacle to public participation in the digital economy, even though consumer trust is the foundation of e-commerce and digital financial services. If the legal system fails to deliver genuine deterrence and adequate protection, that trust will erode and the digital economy's potential will not be optimally realized. Inconsistency in applying the EIT Law is therefore not merely a technical-juridical matter but a threat to the broader socio-economic order.

Prior studies have touched on cybercrime but each leaves a gap. Bunga (2015) focuses on cyber prostitution rather than fraud; Suhariyanto (2020) analyzes cybercrime in general without specifically addressing the construction of criminal liability for online fraud after the amendments; Sitompul (2012) examines the penal framework under the EIT Law before its revision; Raharjo (2016) emphasizes the civil dimension of consumer protection; and Rizal (2019) confines itself to sale-and-purchase fraud. No study has comprehensively analyzed the misapplication of the post-2024 EIT Law by combining a comparative normative analysis of the Criminal Code and the EIT Law with current empirical judicial data in a single jurisdiction. It is this gap the research gap that this study addresses, which also marks its originality.

Two principal questions follow. First, how is the EIT Law concretely applied in enforcing online-fraud offenses within the jurisdiction of Bandung City, viewed from the indictment, evidentiary, and adjudication stages? Second, why does inconsistency arise in applying the EIT Law to online-fraud perpetrators in that jurisdiction, and what factors underlie it? The study aims to analyze the concrete application of the EIT Law at those three stages, identify the factors causing inconsistency, and formulate a more accurate, consistent, and equitable model of application.

METHODS

This is an empirical juridical (socio-legal) study with a descriptive-analytical specification. This type was chosen because the problem under examination inconsistency in applying the EIT Law is phenomenological and can only be fully understood through observation of actual practice, while remaining situated within the prevailing normative framework (Sunggono, 2020). The study operates at the intersection of norms (das sollen) and the reality of enforcement (das sein).

Two complementary approaches are used. The statutory approach examines the Criminal Code (Article 378), the EIT Law in its three versions (Law No. 11/2008, Law No. 19/2016, and Law No. 1/2024), the Criminal Procedure Code (Articles 184 and 98–101), and the Witness and Victim Protection Law. The case approach examines three final and binding decisions of the Bandung District Court and one comparative precedent, Supreme Court Decision Number 2168 K/Pid.Sus/2019 (Marzuki, 2021).

The research site was chosen deliberately. Bandung City is among the metropolitan areas with the highest internet penetration and volume of digital transactions, making it a significant and representative site for observing enforcement practice. The study was conducted across the three core institutions of the criminal justice system the Bandung City Police, District Attorney's Office, and District Court because they directly handle online-fraud cases from investigation through sentencing. This cross-institutional design enables source triangulation: divergent perspectives at each node of the justice chain can be tested against one another and confronted with documentary evidence in the form of decisions.

Primary data were gathered through in-depth interviews with purposively sampled informants: a cyber-unit investigator of the Bandung City Police, a public prosecutor of the Bandung City District Attorney's Office, and a judge of the

Bandung City District Court, each with direct experience handling online-fraud cases (Moleong, 2021). Secondary data were obtained through library research on primary, secondary, and tertiary legal materials. Analysis proceeded qualitatively in four stages data reduction, data display, interpretation, and conclusion drawing with validation through triangulation and member checking to ensure that the findings reflect actual conditions rather than the subjective view of a single informant. The analytical parameters were derived from criminal-liability theory (the rigor of analyzing mens rea and actus reus) and Fuller's theory of legal certainty (the fulfillment of the principles of legality).

RESULTS & DISCUSSION

The Empirical Picture: Three Patterns of Application in Similar Cases

Between 2021 and 2024, the cyber unit of the Bandung City Police received 312 online-fraud reports. Of these, 187 advanced to investigation, 143 were forwarded to the prosecution, and only 98 culminated in final and binding decisions a conversion rate of roughly 31.4%. In other words, nearly 70% of reports did not result in a completed conviction. Most relevant to the research questions is the shift in the legal basis used in indictments: the share of cases charged cumulatively (Article 378 of the Criminal Code in conjunction with Article 28(1) of the EIT Law) rose from 22.2% (2021) to 41.7% (2024). The trend signals a change in officials' posture, yet it does not amount to consistency.

Table 1. Online Fraud Cases at the Bandung City Police, 2021–2024

Year	Reports	Investigated	Forwarded	Final (dominant provision)
2021	64	38	28	18 (Art. 378: 14; Cumulative: 4)
2022	79	47	35	25 (Art. 378: 18; Cumulative: 7)
2023	91	57	48	31 (Art. 378: 19; Cumulative: 12)
2024	78	45	32	24 (Art. 378: 14; Cumulative: 10)
Total	**312**	**187**	**143**	**98**

Source: Bandung City Police data, processed by the author (2026).

The 31.4% conversion rate is itself an indicator of systemic failure that warrants a critical reading. The attrition from 312 reports to 187 investigations, then 143 transfers, and finally 98 final decisions reveals leakage at every node of the criminal justice chain. Each contraction is not a mere administrative statistic but a reflection of concrete obstacles: digital evidence failing the formal standard, files repeatedly returned, and indictments collapsing at trial. The low conversion rate is thus a surface symptom of a deeper problem whose roots are unpacked through the four factors below.

Three cases were purposively selected for in-depth analysis on the basis of differing modus operandi, differing provisions applied, and varying levels of loss.

Together they illustrate three distinct patterns of legal application, even though all three are substantively fraud committed through electronic media.

Table 2. Profile of the Three Cases Studied

Case Number	Modus	Loss	Indictment	Basis of Decision
131/Pid.B/2022/PN.Bdg	Investment scam (47 victims)	IDR 3.2 bn	Art. 378 CC + Art. 28(1) EIT	Art. 378 CC only; 2 years
245/Pid.Sus/2023/PN.Bdg	Fictitious store (32 victims)	IDR 480 m	Art. 28(1) EIT only	Art. 28(1) + 45A(1) EIT; 1 yr 6 mo
312/Pid.Sus/2024/PN.Bdg	Phishing of banking data (28 victims)	IDR 1.1 bn	Art. 378 CC + Art. 28(1) + Art. 30 EIT	Cumulative granted; 3 yr 6 mo

Source: Bandung District Court decisions, processed by the author (2026).

Table 2 reveals the paradox at the heart of this study. The most serious case an investment scam of IDR 3.2 billion with 47 victims received the narrowest legal basis (the Criminal Code alone) and the lightest sentence (two years), whereas a case with a smaller loss (IDR 1.1 billion) received cumulative application and the heaviest sentence (three years and six months). This disparity does not correlate with the gravity of the offense but with the quality of the indictment and the completeness of the digital evidence a finding elaborated in the subsections that follow.

Applying the EIT Law Across the Criminal Justice Chain

Analysis across the four stages investigation, prosecution, proof, and adjudication shows that inconsistency is not an isolated occurrence at one point but a chained, mutually reinforcing weakness (a systemic chain of weakness).

At the investigation stage, cyber-unit investigators rely on the National Police's technical guidance, which treats Article 28(1) of the EIT Law as the principal provision that may be combined with Article 378 of the Criminal Code. In practice, however, the choice of provision is situational shaped by the completeness of evidence, the team's technical capacity, and superiors' direction. The absence of a standard operating procedure for qualifying conduct under EIT Law provisions causes qualifications to vary even where the modus is similar. The complexity of determining the locus and tempus delicti in cross-border crime perpetrator in Bandung, server abroad, victims dispersed, holding accounts registered in another city compounds the problem (Suseno, 2012). The perpetrators' ability to erase digital traces (encryption, unregistered prepaid numbers, money-mule accounts, VPNs) collides with the limited forensic capacity of officials, so digital evidence is often too weak to sustain EIT Law charges (Ramli, 2020).

The technical instruments available at the city-police level forensic imaging of seized devices, platform data extraction through mutual legal assistance (MLA), metadata analysis, and tracing fund flows with the Financial Transaction Reports and Analysis Center (PPATK) face structural limits in practice. Success in obtaining data from foreign platforms depends heavily on corporate policy and international agreements and does not always yield comprehensive evidence. The problem is aggravated by the scarcity of certified digital forensic experts, who are concentrated in major cities; when an expert cannot be presented, digital-evidence analysis tends to be superficial and falls short of the standard needed to sustain EIT Law charges (Makarim, 2021). This dependence on factors beyond investigators' control renders the quality of online-fraud case files highly uneven from the very start.

At the prosecution stage, prosecutors face three indictment constructions: a sole Criminal Code charge, a sole EIT Law charge, or a cumulative charge. Interviews revealed a pragmatic dimension rarely discussed in the literature: prosecutors' decisions are shaped by pressure on the conviction rate. Prosecutors tend not to place the EIT Law as the primary charge when they doubt its elements can be proved, because if the EIT Law charge fails while the Criminal Code charge succeeds, the defendant is still convicted and the success statistics are preserved. This risk-averse logic structurally pushes officials toward the provision that is easiest to prove rather than the one that is most legally appropriate. Analysis of the indictments reinforces this finding: in Case 131/2022 the elements of Article 28(1) were set out in only two paragraphs without adequate elaboration, whereas in Case 312/2024 the prosecutor elaborated the EIT Law elements across more than twenty paragraphs supported by eight items of expert-verified digital evidence. The difference in quality between two prosecutors from the same office underscores the weight of individual capacity.

The absence of prosecutorial specialization worsens the situation. At the Bandung City District Attorney's Office, online-fraud cases are handled by general prosecutors who also handle various other matters, so a prosecutor may be drafting an EIT Law indictment for the first time. Without specific prosecution guidelines, prosecutors effectively “grope” for the right construction in each case producing variation that is in truth unnecessary and avoidable through standardization (Suhariyanto, 2020).

At the evidentiary stage, the most complex problem emerges. Article 184 of the Criminal Procedure Code enumerates admissible evidence exhaustively, while Article 5 of the EIT Law adds electronic information and documents as valid evidence yet the formal and material requirements remain unstandardized. Judges face two challenges: difficulty verifying the authenticity and integrity of the digital evidence presented, and difficulty interpreting the phrase “disseminating false and misleading news.” Amid technical uncertainty, judges tend to set a higher threshold for digital evidence and to apply in dubio pro reo resolving doubt in the defendant's favor which leads to the failure to prove the EIT Law elements even where the conduct substantively satisfies them. The most consistent finding is that the presence of a digital forensic expert is the decisive factor: only Case 312/2024 presented such an expert, and only that case successfully applied the EIT Law in full (Sitompul, 2012).

The evidentiary problem extends beyond the authenticity of digital evidence. One of the most substantive issues is the difficulty of proving "consumer loss in an electronic transaction" as required by Article 28(1). On a narrow reading, the phrase presupposes a consumer–business relationship; yet many online frauds take the form of investment relationships, romance scams, or pyramid schemes masquerading as "community membership" that do not fit the classic sale-and-purchase mold. In Case 131/2022, defense counsel exploited this gap by arguing that the relationship between the defendant and the victims was a civil "investment partnership," so that any loss was a business risk an argument that succeeded in "saving" the defendant from the EIT Law charge even though it was not wholly accepted under the Criminal Code (Sitompul, 2012).

At the adjudication stage, the three cases display divergent patterns. In Case 131/2022, the judge set aside the EIT Law on the view that the defendant's conduct was a "false promise" characteristic of the Criminal Code rather than the "dissemination of false news," which the judge believed required dissemination to the broader public. In Case 245/2023, the judge instead applied the EIT Law in pure form without the Criminal Code. In Case 312/2024, the cumulative charge was granted in full. The divergent patterns in substantively comparable cases constitute the most visible evidence of the inconsistency at issue. It bears emphasizing that the divergence consistently correlates with one variable: the presence of a digital forensic expert and the quality of the indictment's elaboration. Where both are present (Case 312/2024), the EIT Law is fully applied; where absent (Case 131/2022), it falls away. This correlation shifts the locus of the problem from the substance of the norm to the procedural and capacity domains a finding that grounds the argument for standardization in the subsections that follow.

A Critical Analysis of Judicial Reasoning: Misinterpreting "Dissemination"

The judge's reasoning in Case 131/2022 deserves serious scrutiny. The argument that the element of "disseminating false news" was not satisfied because the dissemination targeted specific individuals rather than the unlimited public contains a fundamental interpretive error. Article 28(1) of the EIT Law does not textually require that dissemination be massive or directed at the broad public. A person who systematically promotes a claim of 30% monthly investment returns to 47 victims via social media, while knowing the claim to be impossible, is in fact "disseminating information known to be false" through an electronic platform. The targeted nature of the dissemination does not negate the element of "dissemination" itself (Suhariyanto, 2020).

This error is not merely a technical-juridical matter; it produces a justice gap. Article 28(1) in conjunction with Article 45A(1) of the EIT Law threatens up to six years' imprisonment and/or a fine of up to IDR 1 billion, whereas Article 378 of the Criminal Code threatens only four years. By setting aside the EIT Law, the judge foreclosed the room to impose a sentence proportionate to a loss of IDR 3.2 billion and 47 victims. As a result, the gravest case received the lightest sanction a contradiction that defies the rationality of sentencing. From the standpoint of criminal-liability theory, setting aside the EIT Law also overlooks an essential dimension of the conduct: that this crime specifically exploited an electronic medium to reach a large number of victims with high anonymity (Ramli, 2020).

Teleologically, the purpose of Article 28(1) is to protect the integrity of the electronic transaction ecosystem from information that erodes trust. Confining the element of "dissemination" to mass communication reduces that protection precisely where it is most needed targeted fraud designed personally to maximize success. Such a narrow reading runs counter to the principle that law should be interpreted to achieve its purpose, not to defeat it. Moreover, the inter-case comparison shows that the differentiator of successful EIT Law application is not the substance of the conduct but procedural variables: the quality of the indictment, the presence of an expert, and the completeness of evidence. This is the crux of legal certainty the legal fate of a defendant is determined by the competence of the officials handling the case rather than by the degree of culpability.

The Construction of Criminal Liability in Online Fraud

Criminal-liability theory requires the cumulative fulfillment of actus reus, mens rea, the capacity to be held responsible, and the absence of any excuse (Hamzah, 2019; Saleh, 2013). In online fraud, the actus reus is not a single physical act but a chain of digital actions: creating an account resembling a legitimate entity, posting false claims, sending manipulative messages, receiving funds into intermediary accounts, and using the funds for personal benefit. Collectively, this chain satisfies the actus reus of both Article 378 of the Criminal Code and Article 28(1) of the EIT Law.

Proof of mens rea particularly dolus directus is reconstructed from patterns evincing careful planning: choosing an account name resembling a legitimate company (intent to mislead), using money mules (awareness of unlawfulness), and ceasing communication once funds are received (proof that the promised returns were never intended). On this basis, the present author contends that the decision applying only the Criminal Code in Case 131/2022 is erroneous from the standpoint of criminal-liability construction, because it disregards the digital dimension that is in fact an aggravating feature.

The principle geen straf zonder schuld (no punishment without fault) acquires particular relevance in the digital space. When a perpetrator uses a false identity, a fictitious account, or an unregistered number, proving that this particular person possessed the mens rea becomes far more difficult. The absence of technical guidelines for proving fault in the digital environment is, in the author's view, one of the principal sources of decision inconsistency. Without standards linking digital traces to the perpetrator's intent in a convincing manner, judges are inclined to apply in dubio pro reo and set aside EIT Law charges, even where the conduct substantively satisfies their elements (Permata, 2017).

A thornier dimension is organized online fraud. In the investment-scam case studied, the defendant did not act alone: there were fake "successful investor testimonials," a fund-transfer manager, and a supplier of promotional material yet only the principal perpetrator was charged. The doctrine of participation (deelneming) under Articles 55–56 of the Criminal Code should reach all roles, and the doctrine of joint criminal enterprise can serve as a conceptual foundation for charging every participant who knowingly takes part in a shared criminal scheme. The failure to reach the entire chain of liability is a significant weakness and also opens a discussion of the relevance of corporate criminal liability where a lawful business entity is used as a "shell" for fraudulent operations (Makarim, 2021).

Corporate criminal liability deserves serious consideration when a lawfully established business entity is used as a "mask" of legitimacy to win victims' trust. Not a few investment frauds use the name of a registered company to reassure prospective victims. In such situations, attributing liability solely to the individuals acting on the company's behalf does not reflect the reality of the crime; the corporation itself should be reachable through the corporate criminal liability provisions in various sectoral statutes. Neglecting this dimension means enforcement halts at the front-line perpetrator while the structure that enables the crime remains intact and ready to operate again.

Four Causes of Inconsistency

Through triangulation of interviews, decisions, and the literature, the author identifies four interacting not freestanding factors that explain the inconsistency in applying the EIT Law. This mapping aligns with Friedman's (1975) legal-system theory, which distinguishes legal substance, legal structure, and legal culture.

First, the normative factor. The dualism between the Criminal Code and the EIT Law has not been resolved through legislative harmonization. A single act may satisfy two norms at once (concursus idealis) without a clear conflict rule. The most critical ambiguity lies in Article 28(1): three elements "false news," "misleading," and "consumer loss in an electronic transaction" are open to multiple interpretations. The principle lex specialis derogat legi generali, which should position the EIT Law as the special rule, is not applied consistently. The transition toward the new Criminal Code (Law No. 1/2023), which contains new fraud provisions, adds a further layer of uncertainty. The revisions of the EIT Law in 2016 and 2024 missed the opportunity to provide a clear conflict rule (Marzuki, 2021; Ali, 2022).

The ambiguity is not confined to Article 28(1). Articles 30 (illegal access), 31 (interception), and 35 (manipulation of electronic documents) of the EIT Law are potentially relevant to frauds involving phishing, digital identity forgery, or manipulation of transaction evidence as seen in Case 312/2024. Yet the absence of guidance on when and how these provisions apply cumulatively leaves prosecutors without an adequate framework to build an indictment reflecting the full dimension of the crime. As a result, the complexity of the defendant's conduct is often reduced to a simpler construction for the sake of easier proof.

Second, the human-resource factor. Limited technical capacity is systemic rather than individual. Of the twelve members of the city police cyber unit, only four hold digital forensic certification. Files are frequently returned because digital evidence fails the formal standard. Prosecutors confront EIT Law elements that are "new" and thin on jurisprudential interpretation, while judges acknowledge their dependence on expert testimony. A recruitment and rotation system that has not yet made cyber competence a placement criterion means that individual capacity-building does not produce sustainable systemic improvement (Soekanto, 2021; Widodo, 2014).

Third, the institutional factor. The absence of a regular coordination forum among investigators, prosecutors, and judges causes each institution to develop its own understanding. The protracted file-return (P-19) process and the limited digital forensic laboratory capacity at the city-police level often requiring analysis to be sent to the provincial police prolong investigations and degrade evidence quality.

Following Friedman (1975), sound legal substance (the EIT Law) remains ineffective when the legal structure (inter-agency coordination) does not function.

Fourth, the legal-culture factor. There is a strong tendency among officials to be more "comfortable" with the Criminal Code, tested over more than a century, than with the relatively new and jurisprudence-poor EIT Law. This tendency is reinforced by a performance-assessment system that measures case-clearance and conviction rates rather than the accuracy of the provision chosen. Systemically, the incentives push officials toward the provision that is easiest to prove not the one that is most legally appropriate (Ali, 2022).

These four factors do not operate in isolation but form a mutually locking cycle. Normative ambiguity (the first factor) creates room for discretion that is then filled by limited capacity (the second); limited capacity is aggravated by weak coordination and infrastructure (the third); and these three conditions in turn perpetuate a legal culture that chooses the safest path (the fourth), which itself forecloses the incentive to remedy the preceding factors. Partial intervention revising the norm without addressing capacity and coordination will not break the cycle. A simultaneous response across all four dimensions is required, as formulated in the model in the eighth subsection.

Evaluating Legal Certainty: A Deficit Across Three Basic Values

Tested against the theory of legal certainty, the application of the EIT Law in Bandung City shows a serious deficit. From Kelsen's (1961) perspective, certainty demands the predictability of norms; yet three similar cases produced three decision variants the antithesis of predictability. Tested against Fuller's (1969) eight principles of legality, at least two are violated: clarity (the phrase "false and misleading news" is insufficiently clear) and congruence between official action and declared rule (a gulf exists between the norm declared in force and the way it is actually applied).

From Radbruch's (1950) perspective, the condition produces a simultaneous deficit across three basic values: certainty is low due to decision inconsistency; justice is impaired because comparable conduct receives different sanctions; and expediency is neglected because deterrence weakens and fraud rates remain unchecked. The author underscores a dimension often overlooked, namely procedural certainty: the absence of clear procedures for obtaining, presenting, and testing digital evidence turns each online-fraud case into its own "legal experiment." The comparative experiences of Singapore (the Computer Misuse Act and the Cybersecurity Act) and Malaysia (the Computer Crimes Act 1997) show that periodically updated application guidelines and structured judicial training produce more consistent jurisprudence a lesson relevant to Indonesia (Rosadi & Pratama, 2018; Rahardjo, 2014).

That comparative lesson points to a crucial node: cyber legal certainty does not arise from the completeness of written norms alone but from a standardized application infrastructure updated to track technological change. As Rahardjo's (2014) idea of progressive law emphasizes, a sound legal system is one capable of adapting dynamically to socio-technological change without losing consistency and predictability. The EIT Law, designed in the 2008 era, has lagged behind contemporary digital modus operandi, and the 2016 and 2024 revisions have not resolved the fundamental problem of legal certainty. It is this deficit of procedural

certainty that is most urgent to remedy, because it touches the procedure not merely the substance at the very point where norms meet practice.

Implications for Victim Protection

Inconsistency in applying the EIT Law has direct implications for victim protection. Across the three cases, not a single victim obtained adequate restitution. In Case 131/2022, the IDR 3.2 billion was unrecoverable because the defendant had already spent it, while the mechanism for joining a civil claim for damages to the criminal case (Articles 98–101 of the Criminal Procedure Code) went unused owing to victims' unfamiliarity with the procedure and the absence of seizable assets (Yulia, 2020). Victims thus suffer layered victimization: material loss compounded by disappointment with a legal system. When the EIT Law is not applied where it should be, deterrence weakens and the room for proportionate sentencing closes driving the dark number ever higher as victims choose not to report (Permata, 2017).

The message this inconsistency sends to the public is highly counterproductive: that the legal system is unprepared for digital crime, and that reporting online fraud often yields no recovery. It is this message that erodes trust and, paradoxically, enlarges the dark number. Effective victim protection is therefore inseparable from consistency in applying the provisions: when the EIT Law is applied accurately, the room for proportionate sentencing opens, deterrence strengthens, and if accompanied by additional restitution penalties victim recovery becomes possible. Accordingly, the accuracy of EIT Law application is a matter of substantive justice for victims, not a mere technical formality.

Research Novelty: An Objective and Measurable Model of EIT Law Application

The novelty of this research lies in formulating an objective and measurable model of EIT Law application as an integrative answer to the inconsistency found. The model synthesizes criminal-liability theory, legal-certainty theory, and the empirical findings, and is designed to be embodied in a Supreme Court Regulation (PERMA) or Attorney General's guidelines so as to bind operationally.

Unlike prior research, whose recommendations generally stop at normative appeals “harmonization is needed” or “capacity must be improved” this model offers operational criteria that can be directly tested against concrete cases. Three screening questions form its core: whether the conduct occurred entirely through a medium classifiable as an electronic transaction or interaction; whether there was active manipulation of digital information conveyed to the victim; and whether digital evidence meeting the minimum standard is available. If all three are satisfied, a cumulative charge becomes mandatory rather than discretionary. By converting the determination of the legal basis from subjective judgment into an examination of objective criteria, the model directly targets the root of the inconsistency found in the three cases and forecloses the risk aversion that has distorted the choice of provision.

First, criteria for determining the legal basis. A sole Criminal Code charge (Article 378) should be used only where fraud occurs through a medium that cannot be categorized as an “electronic transaction,” or where digital evidence is inadequate. A sole EIT Law charge should be avoided because it does not provide as complete a construction of the offense as the Criminal Code for repeated or organized fraud. A cumulative charge should be the standard for fraud committed

entirely through an electronic medium, involving the active manipulation of digital information, and/or causing loss in the context of a digital interaction.

Second, a minimum standard of digital evidence: (a) authenticated forensic imaging accompanied by a record meeting the chain of custody; (b) data from the relevant platform or service provider obtained through official procedure; (c) digital forensic expert testimony linking the evidence to the defendant's conduct; and (d) a chronological reconstruction of the communication and transaction flow. Third, a framework for assessing the elements of Article 28(1) affirming that the element of "dissemination" is satisfied regardless of whether the dissemination is public or targeted, so long as verifiably false information is actively disseminated through an electronic platform. Fourth, a Cyber Law Enforcement Coordination Forum at the city/regency level that brings the cyber unit, the prosecution, and the court together periodically to harmonize understanding and review patterns of inconsistency (Friedman, 1975).

Establishing such a forum which can emulate the existing tax-enforcement coordination forum is expected to gradually reduce inconsistency through structured communication among the pillars of the justice system. It bears emphasizing that the four components of the model are mutually supporting and therefore must be implemented in a sustained sequence: harmonization and technical guidelines supply normative clarity; the evidentiary standard and the element-assessment framework translate it into measurable practice; strengthened forensics and training build the capacity to carry it out; and the coordination forum keeps application uniform over time. Neglecting any one component would return the system to the same cycle of inconsistency documented in this research.

The model must also close a long-neglected gap, namely additional penalties and victim recovery. Across the three cases, not a single judge imposed asset forfeiture or restitution, even though both the Criminal Code and the EIT Law permit it. Within the framework of restorative justice increasingly embraced by Indonesia's criminal justice system, the absence of additional penalties is a real shortcoming: the defendant serves a prison term, but the victim obtains no material recovery. The proposed sentencing guidelines should therefore require the explicit consideration of restitution and the forfeiture of criminal proceeds as an integral part of decisions in online-fraud cases (Yulia, 2020).

Finally, the model must be framed within the perspective of progressive law (Rahardjo, 2014): law exists for humanity, so the interpretation of EIT Law elements must be oriented toward the substantive goals of protecting victims and preserving the integrity of the electronic transaction ecosystem, not toward formal compliance with rigid text. Effective enforcement of online fraud is not merely about choosing the right provision but about building a responsive ecosystem trained investigators, skilled prosecutors, knowledgeable judges, adequate forensic infrastructure, and effective coordination.

CONCLUSION

The application of the EIT Law in enforcing online-fraud offenses within the jurisdiction of Bandung City has not been consistent, accurate, or effective. Inconsistency manifests along the entire criminal justice chain: at the indictment stage there is no uniform standard for choosing between the Criminal Code, the EIT

Law, or a cumulative charge; at the evidentiary stage the strength of digital evidence depends on the presence or absence of a forensic expert; and at the adjudication stage three similar cases produced three different patterns, determined more by the quality of the indictment and the completeness of evidence than by the gravity of the offense.

This inconsistency stems from four synergistically interacting factors: the normative dualism and ambiguity between the Criminal Code and the EIT Law; the limited technical capacity of officials; weak institutional coordination and inadequate digital forensic infrastructure; and a legal culture favoring the Criminal Code because of its more established jurisprudence and to avoid prosecutorial risk. On this basis, what is required is the normative harmonization of the Criminal Code and the EIT Law, the issuance of a Supreme Court Regulation and Attorney General's prosecution guidelines, the strengthening of digital forensic capacity and infrastructure, and the adoption of the objective and measurable model for determining the legal basis offered by this study. Without such concrete steps, inconsistency will persist and deepen legal uncertainty as online-fraud techniques continue to evolve.

CONFLICT OF INTEREST

Concerning the research, authorship, and publication of this paper, the author(s) reported no potential conflicts of interest.

ACKNOWLEDGEMENT

We would like to express our gratitude to the Supervisor, Head of Department of law, Dean of the Faculty of Law, Muhammadiyah University of Sukabumi. We also want to express our gratitude to the teachers who have offered to help with every test and training session.

REFERENCES

Ali, A. (2022). Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence) (8th ed.). Jakarta: Kencana.

Bareskrim Polri. (2023). Laporan Tahunan Tindak Pidana Siber Tahun 2022 [Annual Report on Cybercrime 2022]. Jakarta: Mabes Polri.

Bunga, D. (2015). Prostitusi Cyber: Diskursus Penegakan Hukum dalam Pusaran Teknologi Informasi dan Komunikasi. Denpasar: Udayana University Press.

Direktorat Tindak Pidana Siber Bareskrim Polri. (2024). Rekapitulasi Kasus Siber 2023 [Recapitulation of Cyber Cases 2023]. Jakarta: Mabes Polri.

Friedman, L. M. (1975). The Legal System: A Social Science Perspective. New York: Russell Sage Foundation.

Fuller, L. L. (1969). The Morality of Law (Rev. ed.). New Haven: Yale University Press.

Hamzah, A. (2019). Asas-Asas Hukum Pidana [Principles of Criminal Law] (Rev. ed.). Jakarta: Rineka Cipta.

Kelsen, H. (1961). General Theory of Law and State (A. Wedberg, Trans.). New York: Russell & Russell.

Makarim, E. (2016). Pertanggungjawaban Pidana Penyedia Jasa Internet dalam Transaksi Elektronik. Jurnal Hukum Bisnis, 35(1), 19–40.
Makarim, E. (2021). Kompilasi Hukum Telematika [Compilation of Telematics Law] (Rev. ed.). Jakarta: PT RajaGrafindo Persada.
Marzuki, P. M. (2021). Penelitian Hukum [Legal Research] (Rev. ed., 14th printing). Jakarta: Kencana.
Maskun. (2020). Kejahatan Siber (Cyber Crime): Suatu Pengantar (2nd ed.). Jakarta: Kencana Prenada Media Group.
Moeljatno. (2022). Asas-Asas Hukum Pidana [Principles of Criminal Law] (Rev. ed.). Jakarta: Rineka Cipta.
Moleong, L. J. (2021). Metodologi Penelitian Kualitatif [Qualitative Research Methodology] (Rev. ed., 38th printing). Bandung: PT Remaja Rosdakarya.
Permata, R. R. (2017). Perlindungan Hukum Bagi Korban Penipuan Transaksi Elektronik. Jurnal Ilmu Hukum Padjadjaran, 4(1), 55–74.
Radbruch, G. (1950). Legal Philosophy, in The Legal Philosophies of Lask, Radbruch and Dabin. Cambridge: Harvard University Press.
Rahardjo, S. (2014). Ilmu Hukum [Jurisprudence] (8th ed.). Bandung: PT Citra Aditya Bakti.
Raharjo, A. (2016). Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: PT Citra Aditya Bakti.
Ramli, A. M. (2020). Cyber Law dan HAKI dalam Sistem Hukum Indonesia (3rd ed.). Bandung: Refika Aditama.
Rizal, M. (2019). Penegakan Hukum Pidana Terhadap Pelaku Penipuan Jual Beli Online [Undergraduate thesis]. Universitas Islam Indonesia, Yogyakarta.
Rosadi, S. D., & Pratama, G. G. (2018). Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional, dan Nasional. Jurnal Legislasi Indonesia, 15(1), 1–14.
Saleh, R. (2013). Perbuatan Pidana dan Pertanggungjawaban Pidana: Dua Pengertian Dasar dalam Hukum Pidana. Jakarta: Aksara Baru.
Sitompul, J. (2012). Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. Jakarta: PT Tatanusa.
Soekanto, S. (2021). Faktor-Faktor yang Mempengaruhi Penegakan Hukum (16th ed.). Jakarta: PT RajaGrafindo Persada.
Suhariyanto, B. (2020). Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya (2nd ed.). Jakarta: PT RajaGrafindo Persada.
Sunggono, B. (2020). Metodologi Penelitian Hukum [Legal Research Methodology] (15th ed.). Jakarta: PT RajaGrafindo Persada.
Suseno, S. (2012). Yurisdiksi Tindak Pidana Siber. Jurnal Hukum Ius Quia Iustum, 19(3), 360–382.
We Are Social & Hootsuite. (2023). Digital 2023 Indonesia Report. London: We Are Social.
Widodo. (2014). Kejahatan Siber dalam Perspektif Kebijakan Hukum Pidana. Jurnal Hukum Ius Quia Iustum, 21(1), 64–83.
Yulia, R. (2020). Viktimologi: Perlindungan Hukum Terhadap Korban Kejahatan (2nd ed.). Yogyakarta: Graha Ilmu.
Statutes and Regulations

Criminal Code of Indonesia (Kitab Undang-Undang Hukum Pidana).
Law Number 8 of 1981 on the Criminal Procedure Code.
Law Number 11 of 2008 on Electronic Information and Transactions.
Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions.
Law Number 31 of 2014 on the Amendment to Law Number 13 of 2006 on the Protection of Witnesses and Victims.
Law Number 1 of 2023 on the Criminal Code.
Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions.
Court Decisions
Supreme Court of the Republic of Indonesia Decision Number 2168 K/Pid.Sus/2019.
Bandung District Court Decision Number 131/Pid.B/2022/PN.Bdg.
Bandung District Court Decision Number 245/Pid.Sus/2023/PN.Bdg.
Bandung District Court Decision Number 312/Pid.Sus/2024/PN.Bdg.